FIG. 1

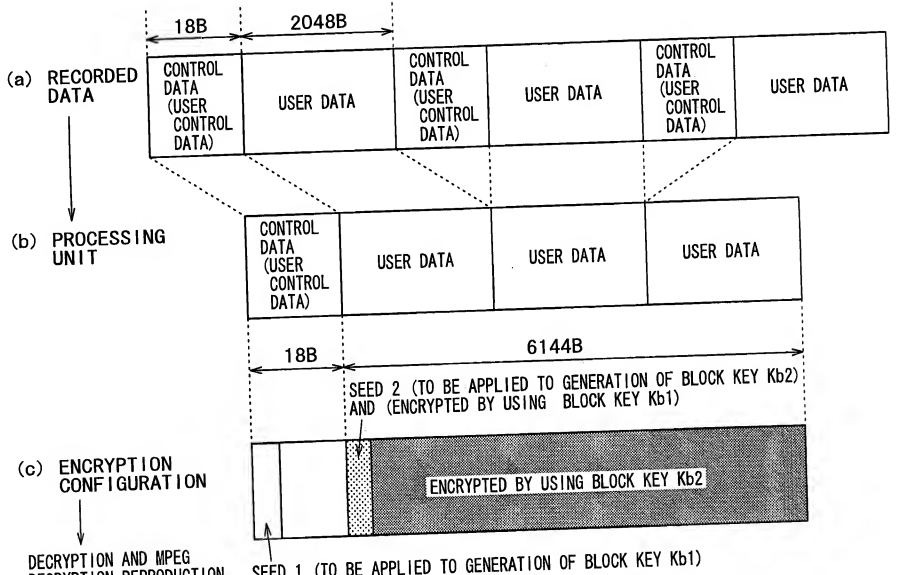


FIG. 2

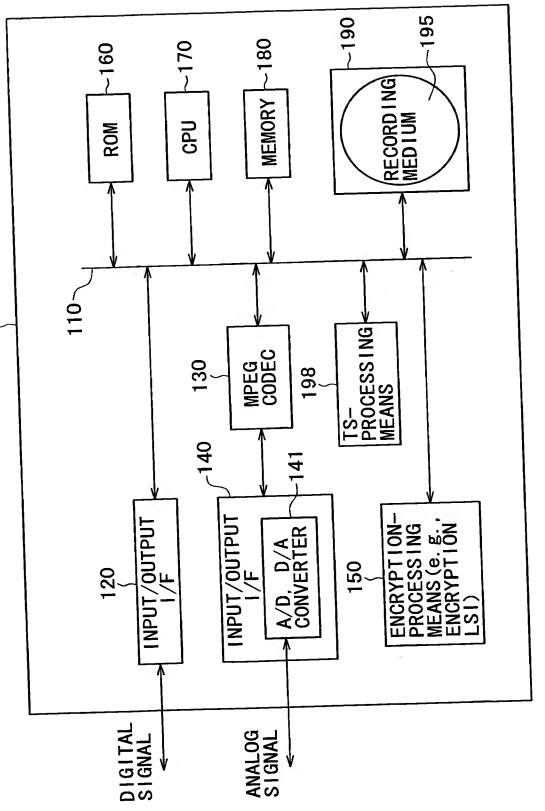

100
110
ROM
160
CPU
170
MEMORY
180
190
RECORDING MEDIUM
195
MPEG CODEC
130
TS-PROCESSING MEANS
198
INPUT/OUTPUT I/F
120
INPUT/OUTPUT I/F
140
A/D, D/A CONVERTER
141
ENCRYPTION-PROCESSING MEANS (e.g., ENCRYPTION LSI)
150
DIGITAL SIGNAL
ANALOG SIGNAL

FIG. 3

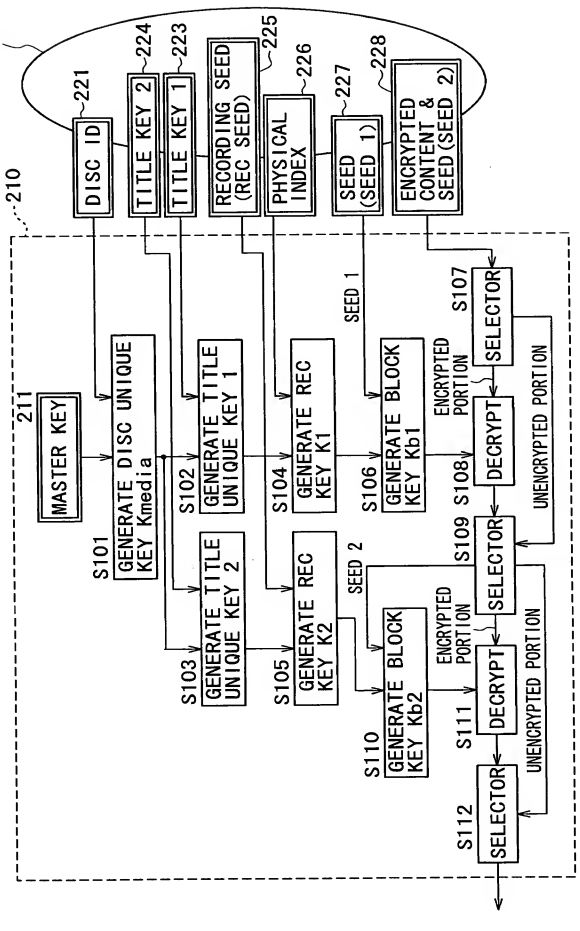

220
210
DISC ID
221
TITLE KEY 2
224
TITLE KEY 1
223
RECORDING SEED (REC SEED)
225
PHYSICAL INDEX
226
SEED (SEED 1)
227
ENCRYPTED CONTENT & SEED (SEED 2)
228
211
MASTER KEY
S101
GENERATE DISC UNIQUE KEY Kmedia
S102
GENERATE TITLE UNIQUE KEY 1
S103
GENERATE TITLE UNIQUE KEY 2
S104
GENERATE REC KEY K1
S105
GENERATE REC KEY K2
S106
GENERATE BLOCK KEY Kb1
S107
SELECTOR
S108
DECRYPT
ENCRYPTED PORTION
S109
SELECTOR
UNENCRYPTED PORTION
SEED 1
SEED 2
S110
GENERATE BLOCK KEY Kb2
S111
DECRYPT
ENCRYPTED PORTION
S112
SELECTOR
UNENCRYPTED PORTION

FIG. 4

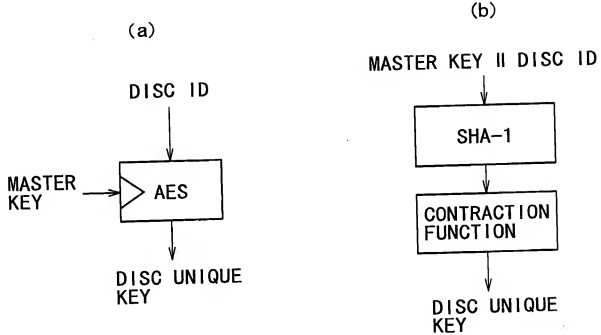


FIG. 5

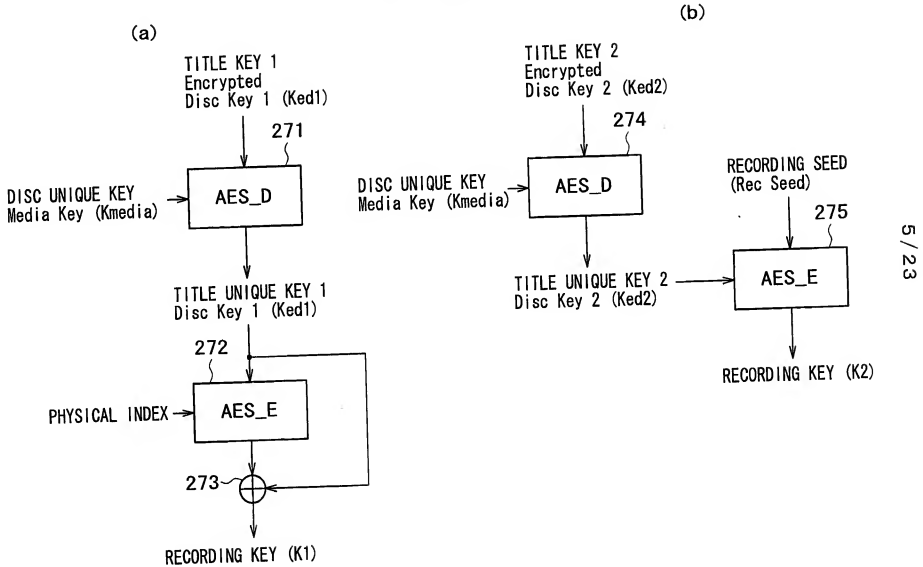


FIG. 6

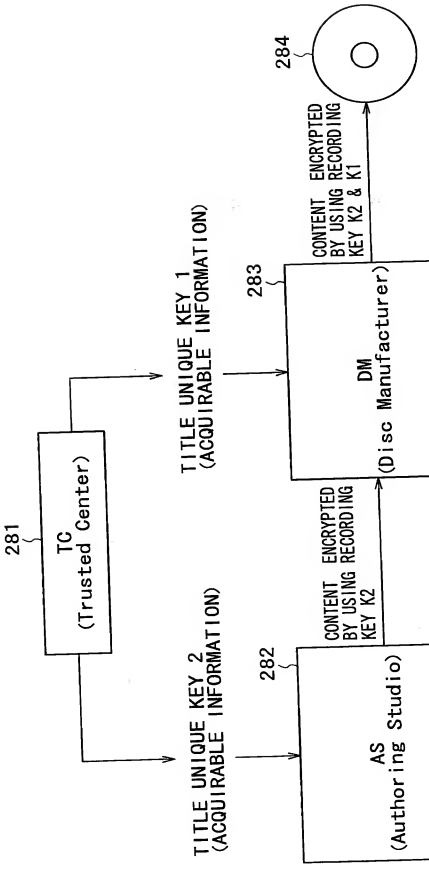

281
TC
(Trusted Center)
TITLE UNIQUE KEY 2
(ACQUIRABLE INFORMATION)
TITLE UNIQUE KEY 1
(ACQUIRABLE INFORMATION)
282
AS
(Authoring Studio)
K2
CONTENT ENCRYPTED BY USING RECORDING KEY K2
283
DM
(Disc Manufacturer)
K1
CONTENT ENCRYPTED BY USING RECORDING KEY K2 & K1
284

FIG. 7

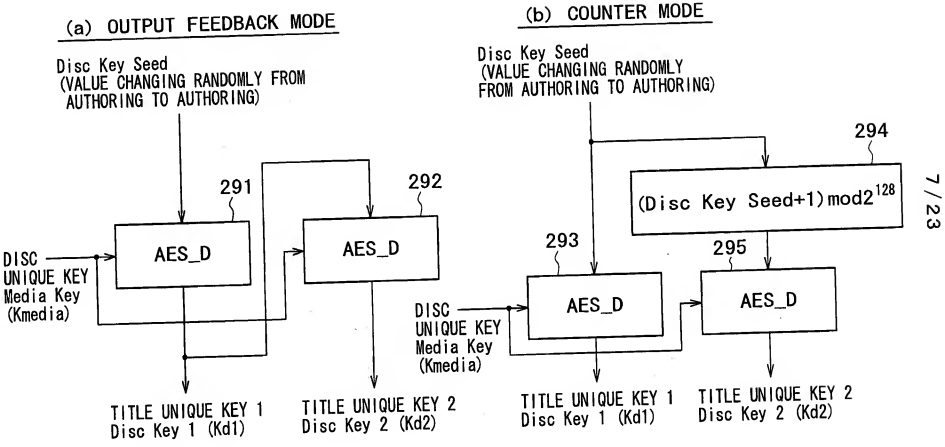


FIG. 8

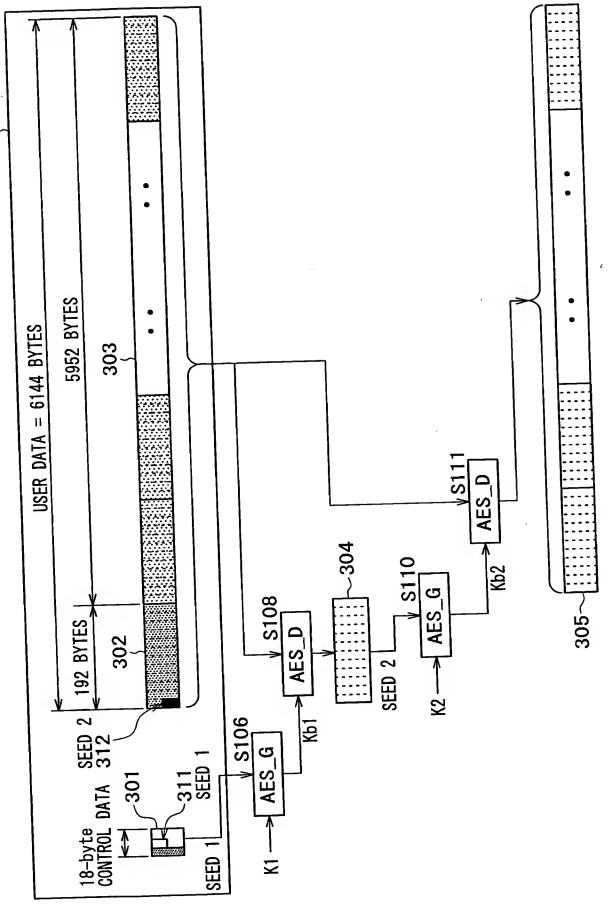

300
USER DATA = 6144 BYTES
5952 BYTES
303
192 BYTES
302
SEED 2
312
18-byte
CONTROL DATA
301
311
SEED 1
SEED 1
S106
AES_G
K1
Kb1
S108
AES_D
304
SEED 2
S110
AES_G
K2
Kb2
S111
AES_D
305

FIG. 9

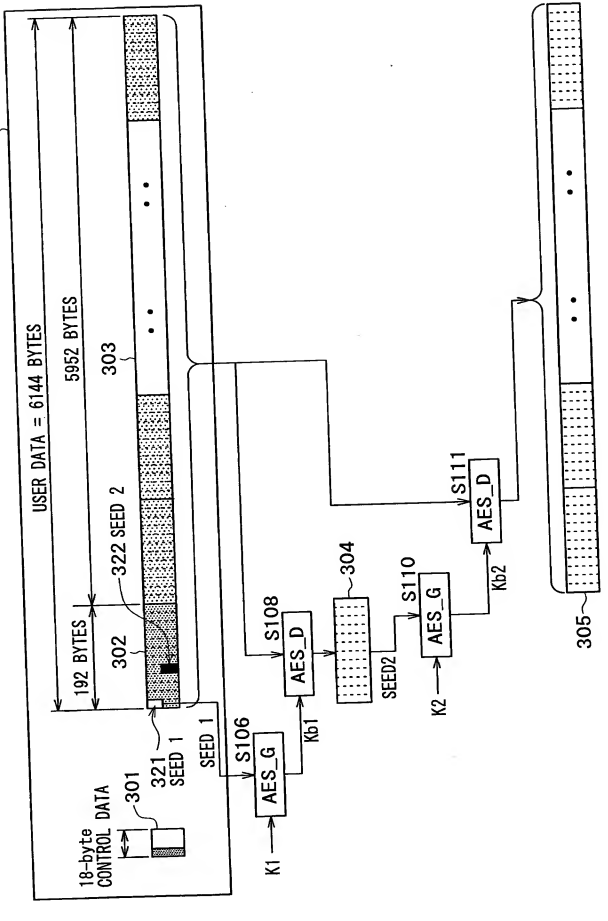

300
USER DATA = 6144 BYTES
5952 BYTES
303
192 BYTES
322 SEED 2
302
18-byte CONTROL DATA
301
321 SEED 1
SEED 1
S106
AES_G
K1
Kb1
S108
AES_D
304
SEED2
S110
AES_G
K2
Kb2
S111
AES_D
305

FIG. 10

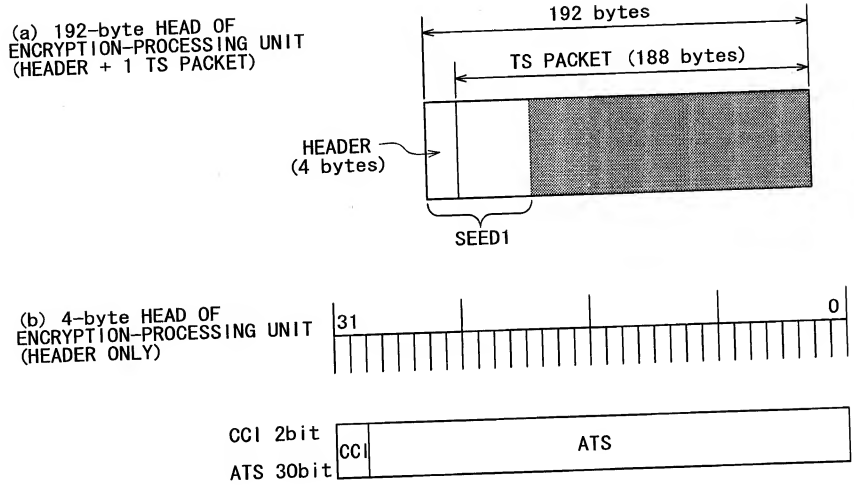


FIG. 11

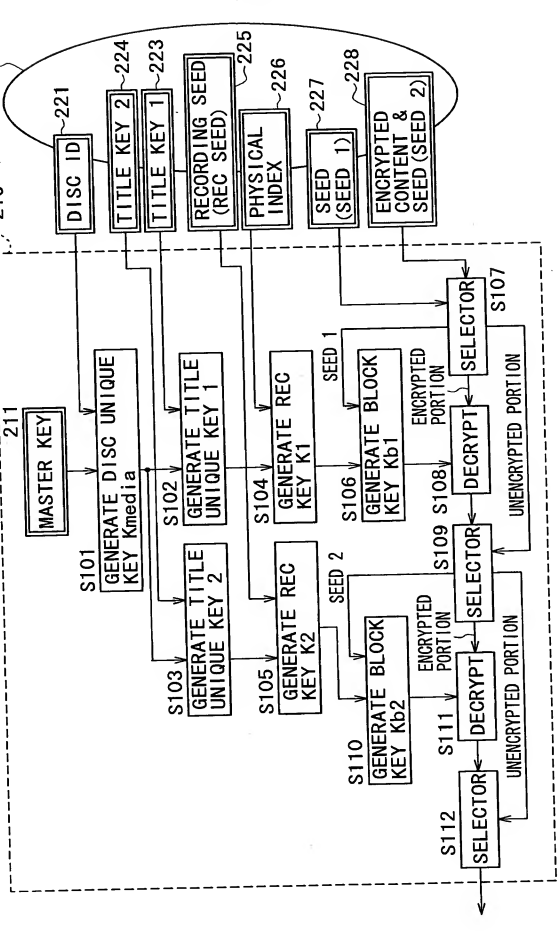

220
210
DISC ID
221
TITLE KEY 2
224
TITLE KEY 1
223
RECORDING SEED (REC SEED)
225
PHYSICAL INDEX
226
SEED (SEED 1)
227
ENCRYPTED CONTENT & SEED (SEED 2)
228
MASTER KEY
211
S101
GENERATE DISC UNIQUE KEY Kmedia
S102
GENERATE TITLE UNIQUE KEY 1
S103
GENERATE TITLE UNIQUE KEY 2
S104
GENERATE REC KEY K1
S105
GENERATE REC KEY K2
S106
GENERATE BLOCK KEY Kb1
S107
SELECTOR
ENCRYPTED PORTION
DECRYPT
S108
SELECTOR
S109
UNENCRYPTED PORTION
SEED 1
SEED 2
S110
GENERATE BLOCK KEY Kb2
S111
DECRYPT
S112
SELECTOR

FIG. 12

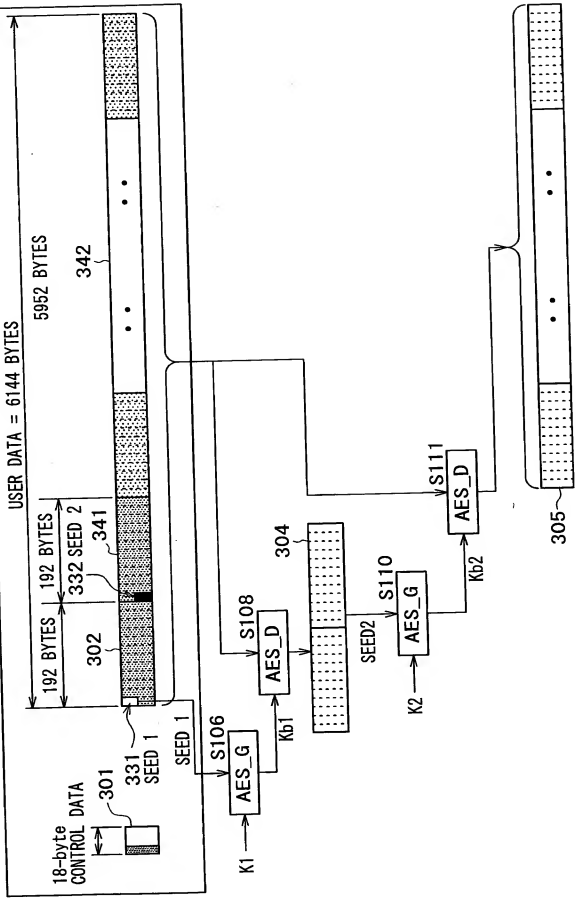

300
USER DATA = 6144 BYTES
5952 BYTES
342
192 BYTES
192 BYTES
332 SEED 2
341
302
18-byte CONTROL DATA
301
331 SEED 1
SEED 1
S106
AES_G
K1
Kb1
S108
AES_D
304
SEED2
S110
AES_G
K2
Kb2
S111
AES_D
305

FIG. 13

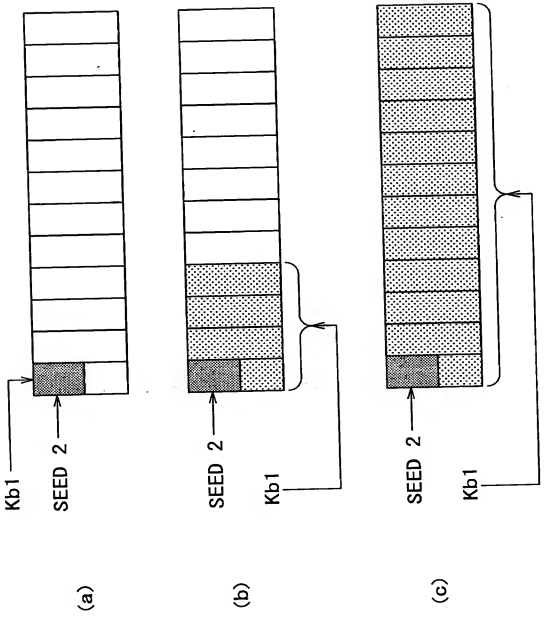


FIG. 14

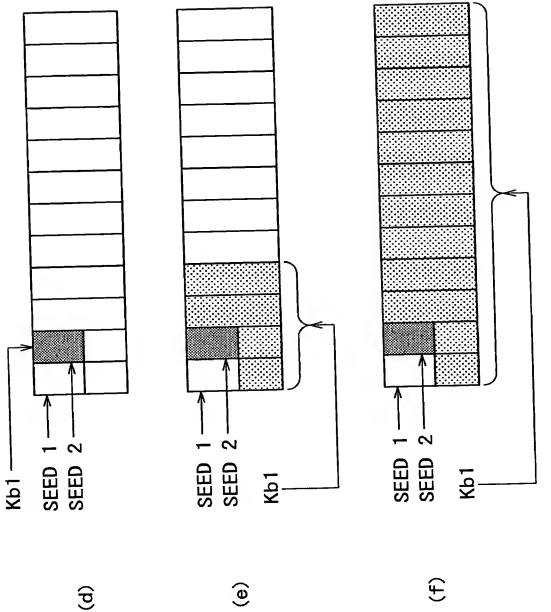


FIG. 15

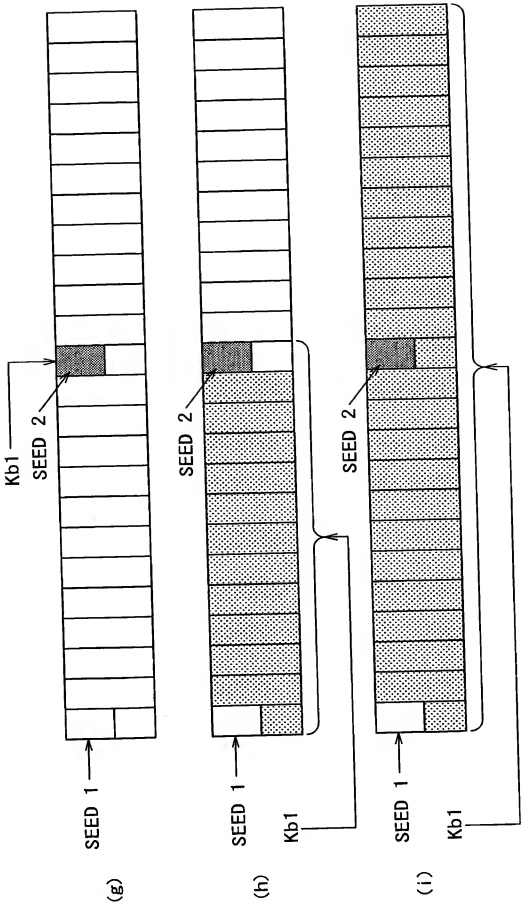


FIG. 16

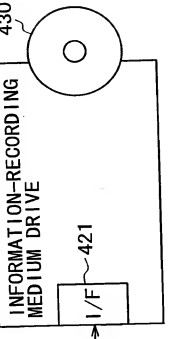

430
420
INFORMATION-RECORDING MEDIUM DRIVE
421
I/F
410
INFORMATION-PROCESSING APPARATUS (SUCH AS PC)
411
I/F

FIG. 17

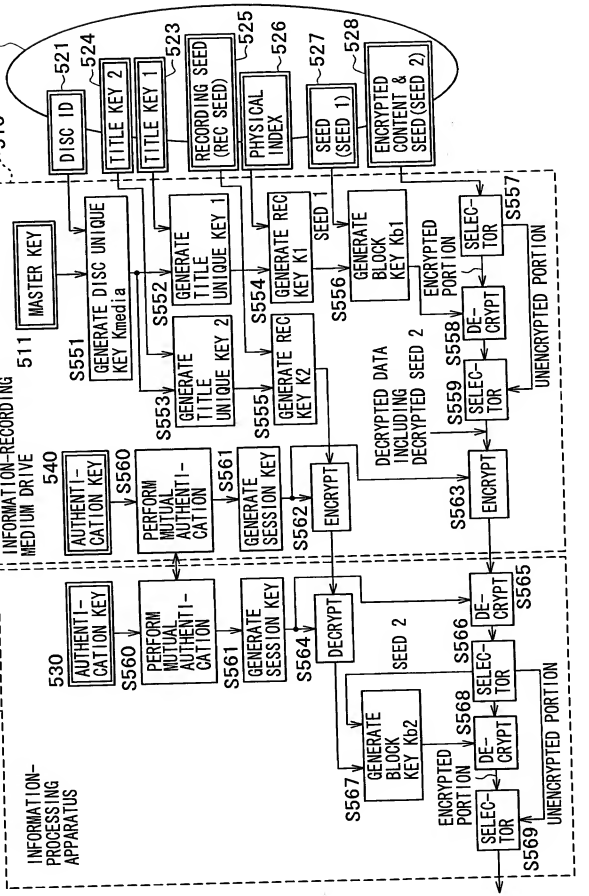

500
INFORMATION-PROCESSING APPARATUS
530
AUTHENTI-CATION KEY
S560
PERFORM MUTUAL AUTHENTI-CATION
S561
GENERATE SESSION KEY
S564
DECRYPT
SEED 2
S567
GENERATE BLOCK KEY Kb2
ENCRYPTED PORTION
S568
DE-CRYPT
S566
SELEC-TOR
S565
DE-CRYPT
SELEC-TOR
S569
UNENCRYPTED PORTION
INFORMATION-RECORDING MEDIUM DRIVE
540
AUTHENTI-CATION KEY
S560
PERFORM MUTUAL AUTHENTI-CATION
S561
GENERATE SESSION KEY
S562
ENCRYPT
S563
ENCRYPT
DECRYPTED DATA INCLUDING DECRYPTED SEED 2
S559
SELEC-TOR
S558
DE-CRYPT
ENCRYPTED PORTION
SELEC-TOR
S557
UNENCRYPTED PORTION
510
511
MASTER KEY
S551
GENERATE DISC UNIQUE KEY Kmedia
S552
GENERATE TITLE UNIQUE KEY 1
S553
GENERATE TITLE UNIQUE KEY 2
S554
GENERATE REC KEY K1
S555
GENERATE REC KEY K2
S556
GENERATE BLOCK KEY Kb1
SEED 1
520
DISC ID
521
TITLE KEY 2
524
TITLE KEY 1
523
RECORDING SEED (REC SEED)
525
PHYSICAL INDEX
526
SEED (SEED 1)
527
ENCRYPTED CONTENT & SEED(SEED 2)
528

FIG. 18

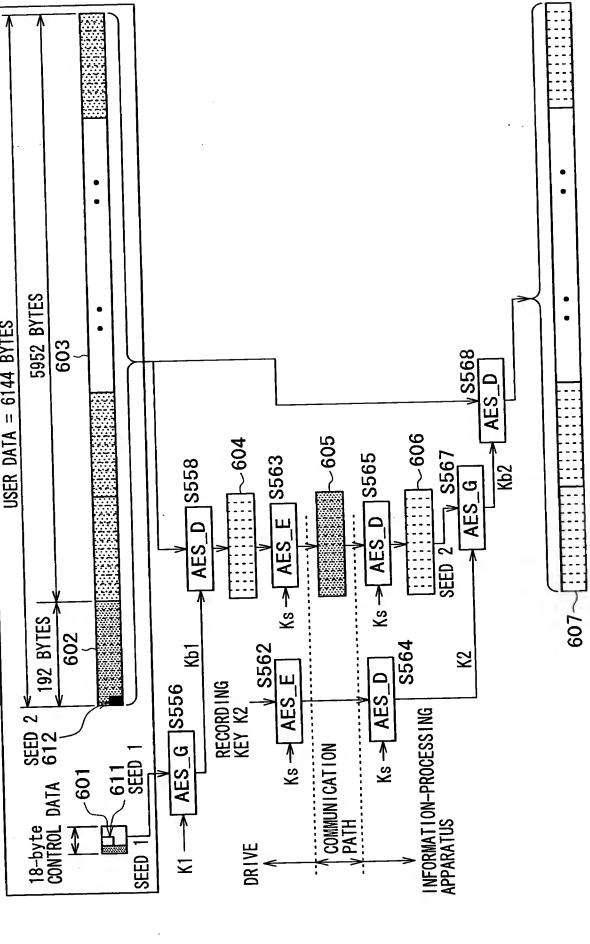

600
USER DATA = 6144 BYTES
5952 BYTES
603
192 BYTES
602
SEED 2
612
18-byte CONTROL DATA
601
611
SEED 1
SEED 1
K1
AES_G
S556
Kb1
AES_D
S558
604
RECORDING KEY K2
S562
AES_E
Ks
AES_E
S563
605
DRIVE
COMMUNICATION PATH
Ks
AES_D
S564
K2
Ks
AES_D
S565
606
SEED 2
AES_G
S567
Kb2
AES_D
S568
607
INFORMATION-PROCESSING APPARATUS

FIG. 19

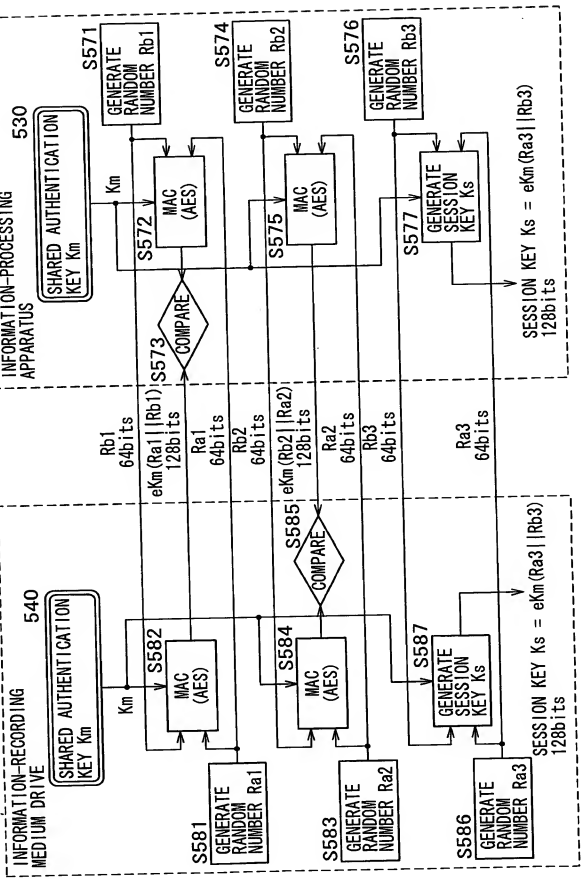

510
INFORMATION-RECORDING MEDIUM DRIVE
500
INFORMATION-PROCESSING APPARATUS
540
SHARED AUTHENTICATION KEY Km
530
SHARED AUTHENTICATION KEY Km
Km
S581
GENERATE RANDOM NUMBER Ra1
S582
MAC (AES)
S583
GENERATE RANDOM NUMBER Ra2
S584
MAC (AES)
S585
COMPARE
S586
GENERATE RANDOM NUMBER Ra3
S587
GENERATE SESSION KEY Ks
SESSION KEY Ks = eKm(Ra3||Rb3) 128bits
S571
GENERATE RANDOM NUMBER Rb1
S572
MAC (AES)
S573
COMPARE
S574
GENERATE RANDOM NUMBER Rb2
S575
MAC (AES)
S576
GENERATE RANDOM NUMBER Rb3
S577
GENERATE SESSION KEY Ks
SESSION KEY Ks = eKm(Ra3||Rb3) 128bits
Rb1 64bits
eKm(Ra1||Rb1) 128bits
Ra1 64bits
Rb2 64bits
eKm(Rb2||Ra2) 128bits
Ra2 64bits
Rb3 64bits
Ra3 64bits

FIG. 20

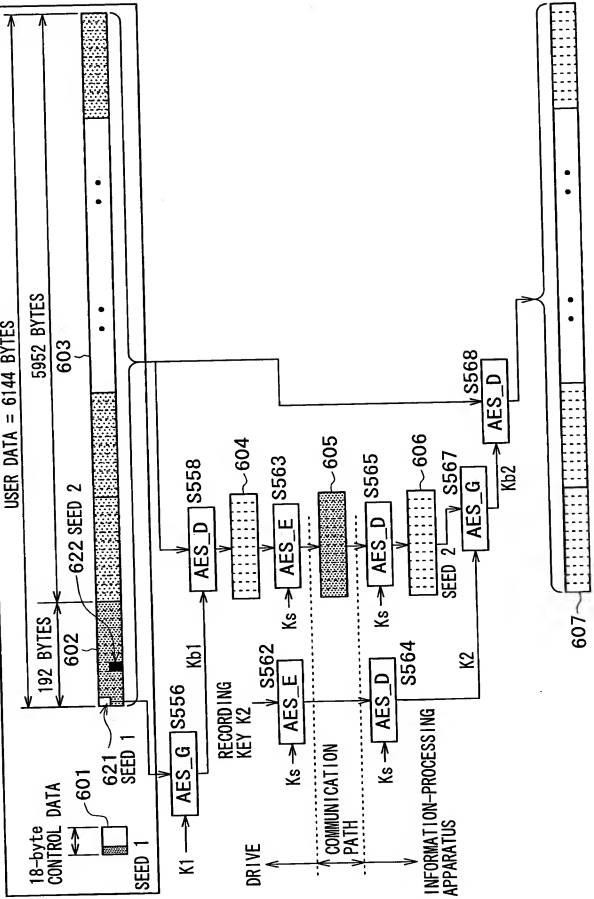

600
USER DATA = 6144 BYTES
5952 BYTES
603
192 BYTES
602
622 SEED 2
18-byte CONTROL DATA
601
621 SEED 1
SEED 1
AES_G
S556
K1
Kb1
AES_D
S558
604
RECORDING KEY K2
AES_E
S562
Ks
AES_E
S563
605
DRIVE
COMMUNICATION PATH
INFORMATION-PROCESSING APPARATUS
AES_D
S564
K2
Ks
AES_D
S565
606
SEED 2
AES_G
S567
Kb2
AES_D
S568
607

FIG. 21

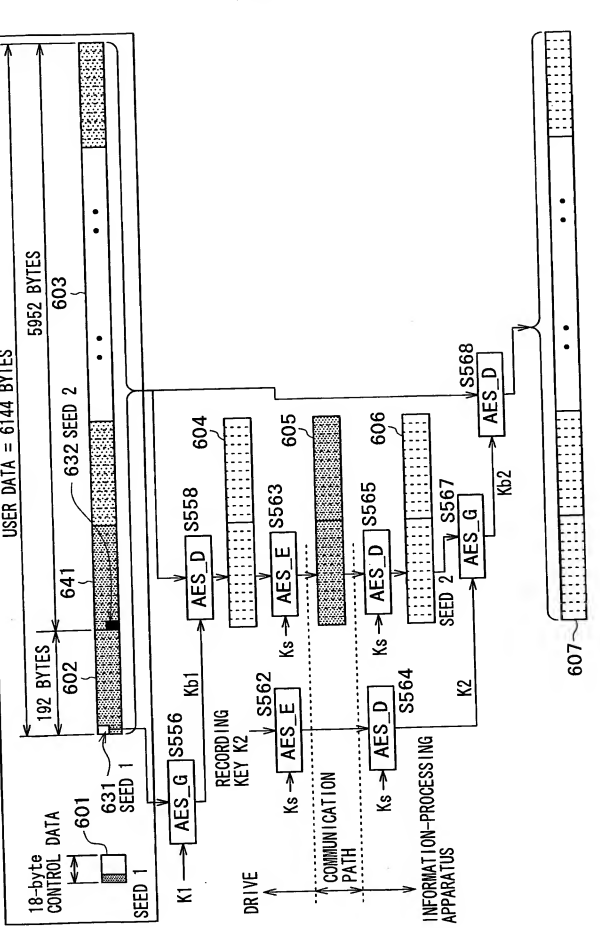

600
USER DATA = 6144 BYTES
5952 BYTES
192 BYTES
602
641
632 SEED 2
603
18-byte CONTROL DATA
601
631 SEED 1
SEED 1
K1
AES_G
S556
Kb1
AES_D
S558
604
RECORDING KEY K2
AES_E
S562
Ks
AES_E
S563
605
DRIVE
COMMUNICATION PATH
Ks
AES_D
S564
K2
Ks
AES_D
S565
606
INFORMATION-PROCESSING APPARATUS
SEED 2
AES_G
S567
Kb2
AES_D
S568
607

FIG. 22

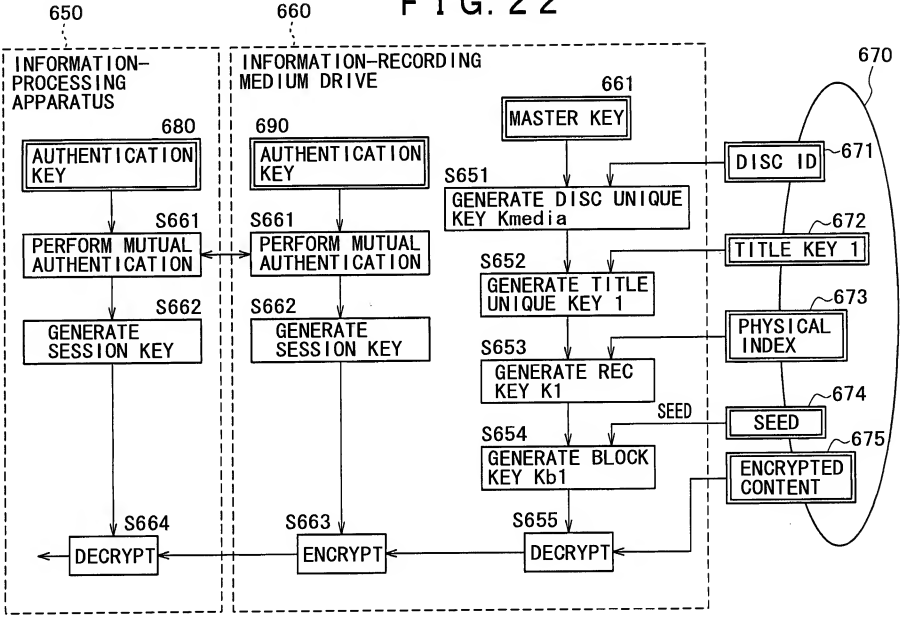
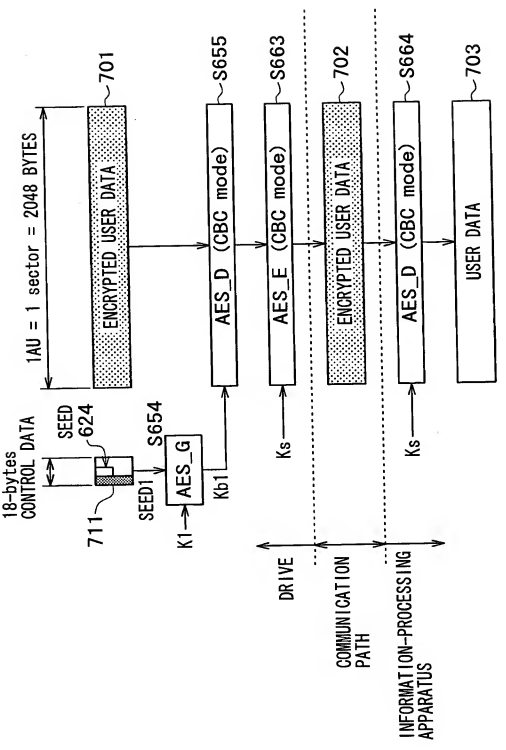


FIG. 23


18-bytes CONTROL DATA
SEED 624
711
SEED1
S654
AES_G
K1
Kb1
1AU = 1 sector = 2048 BYTES
ENCRYPTED USER DATA
701
AES_D (CBC mode)
S655
AES_E (CBC mode)
S663
Ks
Ks
ENCRYPTED USER DATA
702
AES_D (CBC mode)
S664
USER DATA
703
DRIVE
COMMUNICATION PATH
INFORMATION-PROCESSING APPARATUS